Informatica™

Data Privacy by Design

An Agile Approach to Reduce Privacy Risk and Earn Customer Trust

Introduction

The New Data Landscape: More, Faster, Further

Explosive data growth is a double-edged sword. On one hand, it's enabling the most disruptive and exciting companies in the world to create competitive advantages and develop brand new products and services.

On the other, you have to deal with more sensitive data than ever before. And protecting and governing this data is an increasingly complicated challenge.

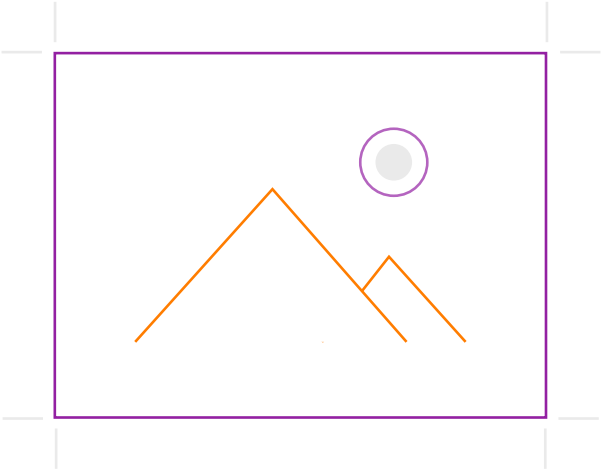
It's not just the volume of data that's causing problems. The speed at which data moves around and between organizations is also increasing. And the data itself is evolving. The purpose, quality, and location of any data asset can change overnight.

This perfect storm of constant change, accelerating speed, and surging volume is creating staggering levels of risk:

- In addition to your traditional structured data in transactional applications and relational databases, there are IoT and social media data streaming into data lakes.
- The desire to use data for analytics, process improvements and machine learning increases the risk of unintentionally using, copying, and combining data in ways that violate consent and regulations.
- Ethical use of data is influencing your customers' decisions on what companies they do business with.
- The sophistication of threat actors and level malicious activities both inside and outside of your business are accelerating.
- And the number of data privacy regulations around the world are growing, and so are the associated fines for non-compliance.

Traditional security and protection models simply aren't fit to address these challenges. What used to be a point-in-time activity is now a continuous process that must be adapted in line with shifting priorities and emerging threats.

This calls for a new paradigm.



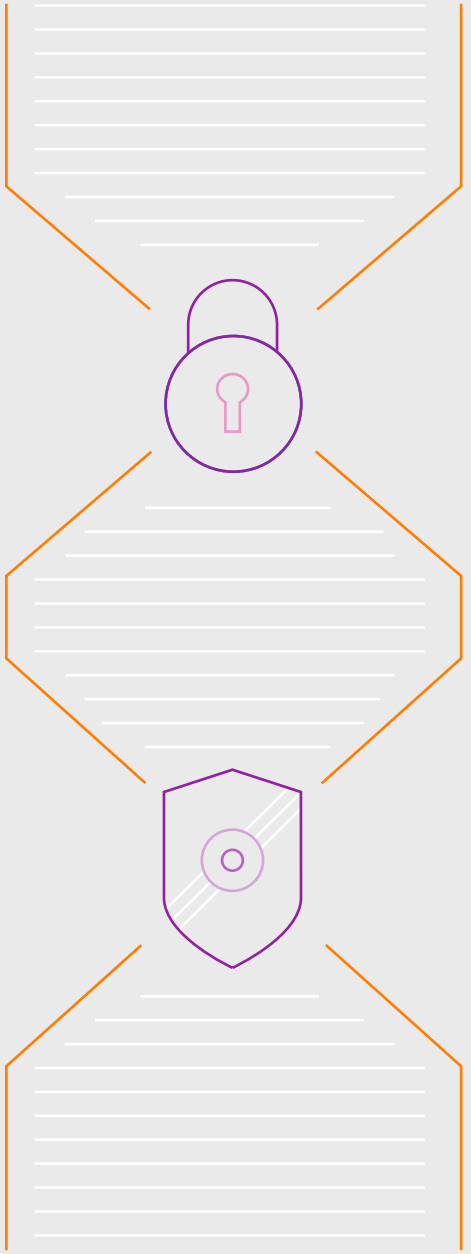
Data privacy must be woven into the DNA of the organization. It must be applied on an enterprise-wide scale and it must involve everyone—because everyone uses data.

This guide explains what this new, holistic approach to data privacy looks like and how you can meet the challenges of a shifting threat landscape.

It's based on our experience working with dozens of enterprise CISOs, Privacy Officers, CDOs, and CIOs on the frontline of data security and protection, as well as our own extensive knowledge of data security intelligence and protection technology.

By the time you've finished reading, you should have a much clearer idea of what effective data privacy looks like today and how you can implement it within your own enterprise.

Let's dive in.



Part One: The perfect storm for data privacy

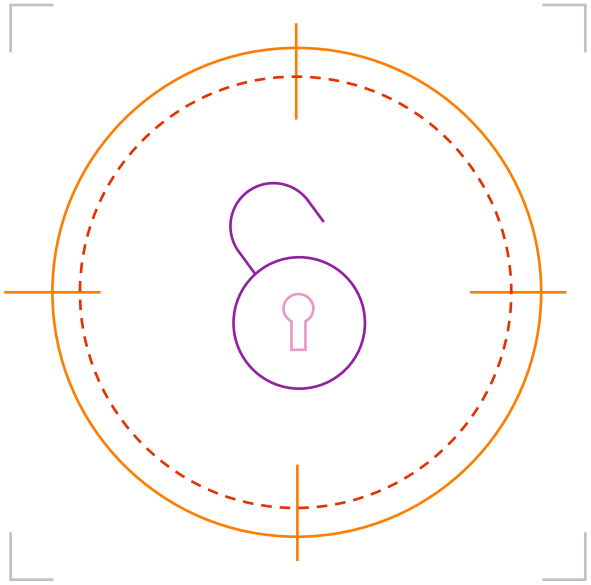
What We Mean When We Talk About Sensitive Data

There are dozens of ways to define personal or sensitive data, but for the purpose of this eBook we'll be talking about Personally Identifiable Information (PII), Payment Card Industry (PCI) and Personal Heath Information (PHI).

Privacy regulations focus on PII, which is a catch-all term for any data that can be used to identify someone. In fact, GDPR has named 60 elements that meet this criteria, including personal, demographic, financial, and health data.

Sensitive data is targeted because it's valuable. Malicious actors can use it to compromise bank accounts and access other valuable datasets. For example, a hacker can use someone's email address to find their phone number. Then, once they have that, they may have enough data to hack the victim's email account.

Leaking this data comes with severe penalties—regulatory fines, legal action, and reputational damage. Of these, reputational damage is perhaps the most daunting. Trust is the cornerstone of every successful customer relationship and once it's broken, it can be incredibly hard to rebuild.



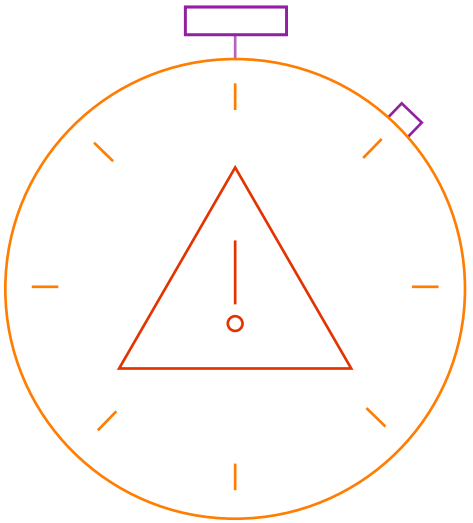
An urgent problem

Data loss has always been an issue for companies, but there are several factors that make it a particularly pressing issue today.

First, more data is being lost than ever before. In 2017, the number of data records compromised in publicly disclosed data breaches surpassed 2.5 billion, up 88 percent from 2016[1]. And there is significant consumer backlash to data breaches.

- 69 percent of global consumers are prepared to boycott any company they believe does not take data protection seriously.
- 62 percent blame the company first in the event of a data breach, rather than the hacker.
- 83 percent of U.S. consumers will stop spending for several months after a breach or serious incident.
- 21 percent of U.S. consumers will never return to a brand that has suffered a data breach.

This spike in breaches and consumers' reactions to breaches is creating an environment where data protection and security is not just a compliance issue but a business imperative.



[1]Gemalto, Breach Level Index 2017, 2017

In the last year alone:

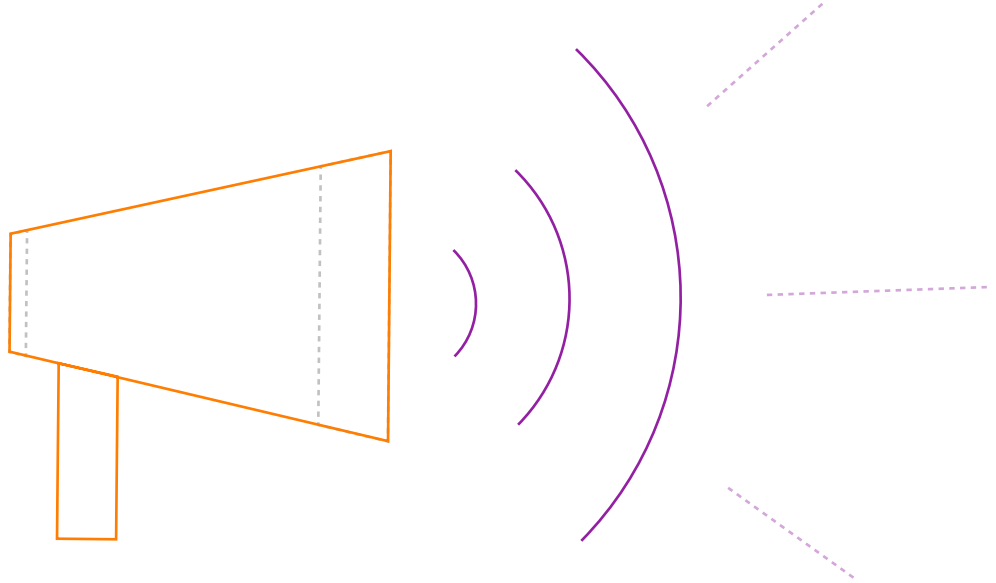
- **GDPR finally came into effect**
  The monumental European Union regulation raised the stakes with staggering fines and a list of stringent rules that will disrupt business as usual.

- **Legislators have taken action**
  More than 80 countries have data privacy laws, and Turkey, India, China, Brazil, Singapore and other countries are clamping down on data security malpractice and rigorously enforcing national and regional laws regarding PII, PCI and PHI. And 11 U.S. states passed or updated privacy laws in 2018.

- **Data privacy has gone mainstream**
  High-profile data breaches and stories of data misuse have made data privacy front-page news. Customers are increasingly interested in how businesses use their data and mistrust enterprises that don't have clear policies.

What used to be an IT concern is now an urgent issue for customers as well as your board, your partners, and regulators.

This puts pressure on you and your team but it also creates opportunities. There are clear business benefits to embracing data privacy.



Digital transformations move faster

Data privacy and governance programs give you the opportunity to establish a data foundation for digital transformation. They help you discover where data resides across the organization. Understand the processes, systems, and people that use the data. And create policies and business rules for quality, protection and use of the data.

These discovery, cataloging, mapping, and governance activities are beneficial to digital business initiatives such as:

- Analytics and Machine Learning—less time required for data scientists to find and cleanse data.
- Business Process Optimization—simplified and automated data exchange between systems.
- Customer Experience—increased understanding of the relationship between customers, products, and commerce channels.

Customer relationships improve

People want to buy from organizations that are demonstrably taking data privacy seriously. According to Capgemini, 77 percent of consumers consider cybersecurity and data protection when choosing a retailer[2] and 27 percent say they'll pay more for better security and privacy features[3]

Few businesses are meeting this demand. Only 25 percent of consumers believe companies handle sensitive personal data responsibly.[4]

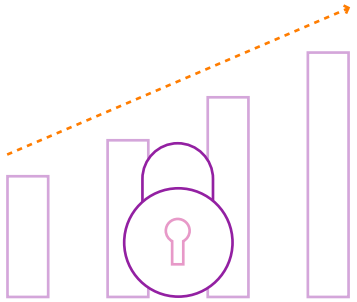
The opportunity here is clear. Prove your ethical data privacy credentials through strong policies and a clean record, and you'll earn all-important trust that forms the foundation of longstanding customer relationships.

[2]Capgemini, Cybersecurity: The new source of competitive advantage for retailers, 2018
[3,4]PwC, Revitalizing privacy and trust in a data-driven world, 2018

Insurance costs fall

Cyber insurance companies integrate data security into their actuarial analysis. Privacy by design and data governance programs help you demonstrate a strong risk management posture that can lower your premiums.

These are just a few examples. The bottom line is that data privacy is not just a compliance issue, it's a business imperative for any company that wants to stay competitive.



Part Two: Know and protect your data

The Challenge of Sustainable Privacy

Until relatively recently, data protection and security was a point-in-time activity that involved protecting a well-defined perimeter. This approach no longer works. Privacy by design requires continuous protection at the asset level. There are four major reasons for this:

1. Your data is everywhere

It's shared across your business and hidden in silos that can be hard to access. It's also creeping outside the traditional perimeter of your business through cloud providers like AWS and Azure, and into third-party SaaS applications that users need.

2. Your data is being used in new ways

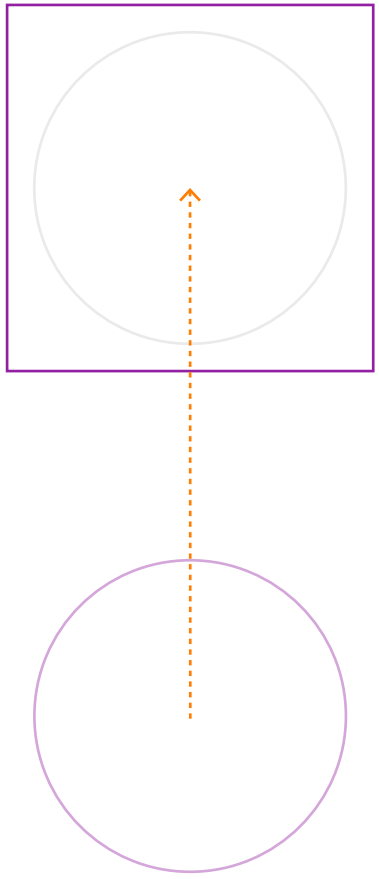
The number of departments, functions, and employees using data for reporting, analytics, new applications, and services is growing rapidly. And people—whether maliciously or accidentally—are your biggest security threat.

3. Your data is growing

Data is flooding into your business and this deluge is only going to increase. Many large organizations handle a petabyte of data and gain an additional terabyte of new information every month. Roughly 30 percent of this data is sensitive.

4. Your data is accelerating

It's becoming easier to share huge quantities of data between different systems at the click of a button, or a tap of a finger. And social engineering has proven incredibly effective at outmaneuvering traditional security measures.



An urgent problem

As we've seen, you're dealing with a huge volume of data that's moving faster and further than ever before. If you can apply security controls at an asset level, then you can protect data wherever it resides, even if it leaves the confines of your organization.

Make no mistake, delivering an effective data privacy program is challenging, but it's not insurmountable. With the right people, processes, and technology, you can address the problems listed above and prepare yourself for an uncertain future.

The following six steps are based on our experience working with dozens of enterprise CISOs, Privacy Officers, CDOs, and CIOs on the frontline of data security and protection, as well as our own extensive knowledge of data security intelligence and protection technology.

1. Define policies and rules

Understand the purpose, use, systems and people related to the processing of personal and sensitive data. This helps you build privacy policies, assign accountability, and provide transparency for consent management activities.

2. Discover and classify

Find personal data across the organization, wherever it exists, and classify its sensitivity and importance based on internal policies and external regulations. Identify data transfer across regulated geographies and understand the regulatory requirements based on region.

3. Map identities

Identity is core to privacy. Personal and sensitive data must be accurately and holistically linked to the individuals it represents in various systems. This helps you address data subject access rights, and data breach notification requirements.

4. Analyze risk

Model and evaluate the privacy risk based on data stores, locations and policies. This helps you plan and prioritize risk remediation across functions, geographies and lines of business.

5. Protect and respond

Implement access controls, and security mechanisms such as encryption, anonymization, and pseudonymization. Track and monitor data use and movement of data. Automate consent management and data subject rights requests.

6. Measure and report

Track compliance and risk indicators to align privacy strategy and operations. Provide dashboards that increase transparency and drive cross functional collaboration and accountability. Automate collection and collation of information for audit reporting.

For these capabilities to be effective, they must be continuous as data, and its use, are constantly changing. They should be integrated, so that privacy and security professionals get a clear and unified view of risks and threats. And they need to be scalable to support the organization as it grows and expands operations. Given the volume of data, users and applications to scan and protect, automation is key not only to keeping pace, but to ensure predictable and reliable results.

And with the growing number of privacy laws and regulations, centralized management will help ensure that organizational policies and guidelines are applied in a consistent manner and simplifies change management. With a broad set of consumers for privacy information and status, a highly visual solution helps simplify the communication of complex information to technical and business professionals.

Of all these qualities, automation is key. You have millions of data points you need to protect, and manual processes can only stretch so far before becoming too time-consuming and expensive. Often, these processes are so slow, they're rendered obsolete long before they're completed.

Automating controls, by establishing policies and tracking metadata, is a far more sustainable way to retain control and visibility in a fast-changing environment.

This sounds daunting, but it really is a simple process. Artificial intelligence is now sophisticated enough that data security intelligence and protection tools can leverage "intelligent" privacy policies and apply them in real time.

In practice, these systems can monitor new and existing data and notify appropriate stakeholders (such as privacy teams) if they spot an anomaly. They can also suggest or take corrective actions to block threats.

In these scenarios, the threat is addressed regardless of its origin. It is about protecting the data itself and detecting patterns of access or behavior by users that indicate inappropriate or unauthorized access.

This is the true power of automation. It doesn't just make life easier for privacy and security experts by automating manual processes, it actively improves security and makes what was formerly impossible, achievable.

Don’t compromise on access

New data protection and privacy regulations have placed fresh emphasis on the importance of making PII accessible.

Under GDPR, you need to be able to delete, move, or amend customer data in line with customer demands. You’ll also need to honor customer requests to withdraw or grant consent.

This means that security measures must be built with a focus on granular access that meets the needs of users based on their role, location, and time of access. There’s no point in ramping up security around sensitive data to such an extreme that no one can adjust consent or share data with a customer.

Take a phased approach

Because the scale of challenges to data privacy and protection is huge, you shouldn’t attempt to tackle everything all at once. Not only is this approach unrealistic but, more importantly, it’s dangerous. The further you stretch your security capabilities, the more likely it becomes that something will slip through the net.

A phased program makes more sense. Start off with your most sensitive data, a small group of people, and a clear objective. Then once you’ve achieved demonstrable results, you can scale your program to tackle new challenges.

First, you’ll need to define “sensitive data.” Risk scoring frameworks can help here. Essentially, you determine a series of criteria that constitute sensitive data and then score data assets on a sliding scale. This approach gives you a nuanced view of data sensitivity and provides consistency and objectivity to the process of defining sensitive data.

It also accounts for the transient nature of data. If one characteristic of a data asset changes—say, its location, usage, or proliferation etc.—its risk score can be adjusted accordingly.

Many of the criteria behind your framework will be unique to your business. But here are a few questions to guide your thinking:

- What type of data are we using and for what purpose?
- What legislation regulates our use and security requirements?
- Who are the business and technical owner of the data?
- How frequently is the data accessed, and is access controlled?

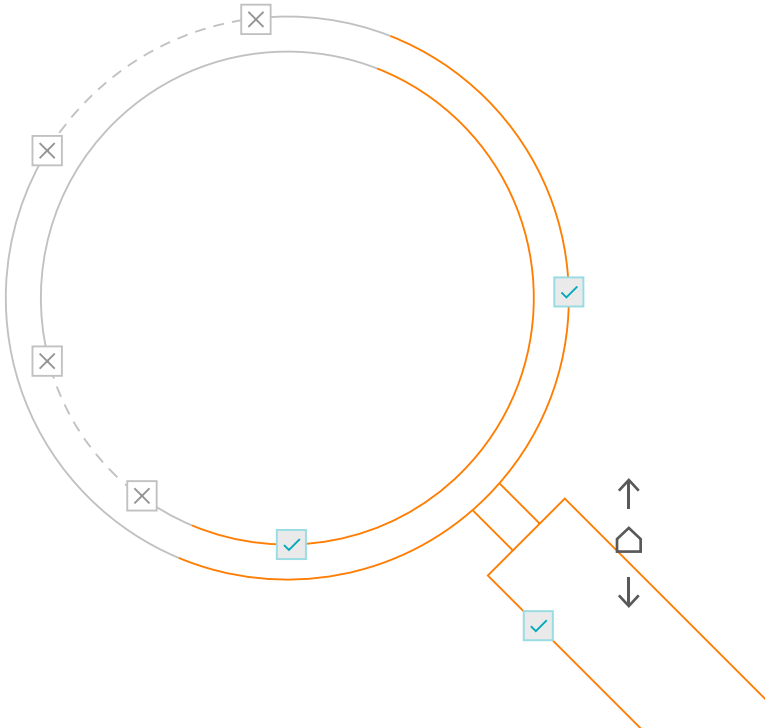
You probably won't be able to answer these questions alone, so you'll need to reach out to the people who use this data on a daily basis. Conducting interviews, surveys, and assessments with application owners, security analysts, DBAs, business analysts, and frontline staff, will expose data types and shed light on user roles, data owners, and business uses.

Once you've defined your data, you can then use automation to discover and classify it. More importantly, you can use risk scoring to determine priorities based on how the data is used, where it travels, and how it is protected.

This process will help you map data across business processes, geographies, and functional groups. It will also provide you with answers to critical questions, such as:

- Where is personal data located, and how is it linked across sources?
- What are the potential risks and are my data protection controls adequate?
- Is the organization's privacy readiness sufficient for the geographies where it operates?
- Have I aligned privacy investments and resources to the right strategic objectives and operational activities?

The answer to these questions will indicate the actions you need to take. So, if the real risk to your data is user error, the action may be to implement a training program.

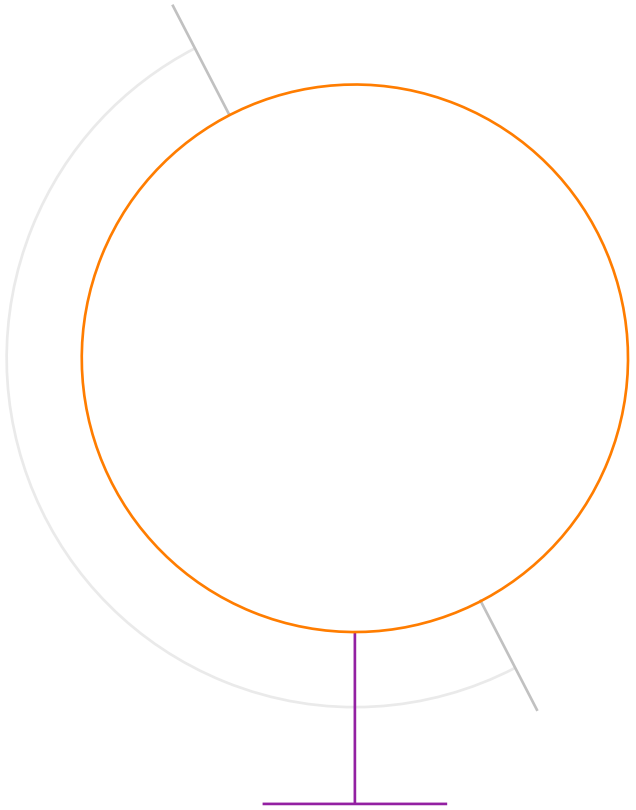


Conclusion

Data Privacy is a Business Imperative

Although market forces are fueling data privacy regulations, it's important to remember that it's not just about compliance. The strong data governance and protection policies and programs required by legislation will also materially impact business success. Your customers, employees and partners expect you to handle their data ethically and responsibly. And digital transformation efforts are dependent upon data to identify new revenue opportunities, streamline business processes, reduce costs, and manage risk.

While the task can seem daunting at first, taking a phased approach and using our six step methodology will help you think big, start small and scale fast. New technologies can help automate tasks, increase transparency, and orchestrate collaboration continuously and with precision. With a holistic approach and a unified technology strategy, you can be ready for the constantly evolving data privacy landscape.

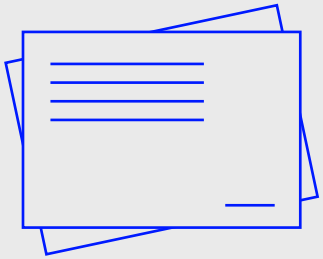


Further Reading

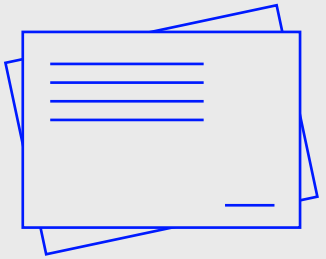
Additional resources/reading

Data Privacy and Protection Video

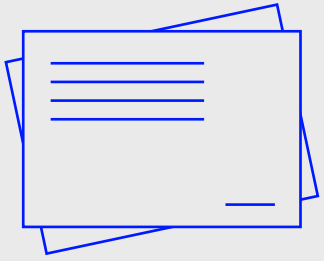
GDPR for Dummies



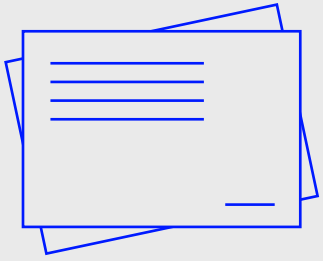
Secure@Source Data Sheet



Data Privacy and Protection White Paper



Data Masking Data Sheet



About Informatica

Digital transformation changes expectations: better service, faster delivery, with less cost. Businesses must transform to stay relevant and data holds the answers.

As the world's leader in Enterprise Cloud Data Management, we're prepared to help you intelligently lead—in any sector, category or niche. Informatica provides you with the foresight to become more agile, realize new growth opportunities or create new inventions.

With 100 percent focus on everything data, we offer the versatility needed to succeed.

We invite you to explore all that Informatica has to offer—and unleash the power of data to drive your next intelligent disruption.

For more information:
Worldwide Headquarters
2100 Seaport Blvd, Redwood City, CA 94063, USA
Phone: 650.385.5000
Fax: 650.385.5500
Toll-free in the US: 1.800.653.3871

www.informatica.com
linkedin.com/company/informatica
twitter.com/Informatica
facebook.com/InformaticaLLC/

CONTACT US

IN19-0119-3582

Informatica™